

Congressional Budget Submission

U. S. Department of Justice

FY 2011 Performance Budget

**Justice Information Sharing Technology  
(JIST)**

## Table of Contents

	Page No.
<b>I. Overview.....</b>	<b>3</b>
<b>II. Summary of Program Changes.....</b>	<b>4</b>
<b>III. Program Changes by Decision Unit to Strategic Goal.....</b>	<b>5</b>
<b>IV. Appropriations Language and Analysis of Appropriations Language.....</b>	<b>6</b>
<b>V. Decision Unit Justification</b>	
A. Justice Information Sharing Technology.....	7
1. Program Description .....	7
2. Performance Tables.....	14
3. Performance, Resources, and Strategies.....	16
a. Performance Plan and Report for Outcomes .....	16
b. Strategies to Accomplish Outcomes.....	17
c. Results of Program Assessment .....	18
<b>VI. Program Increases by Item</b>	
A. Litigation Case Management System (LCMS) ... ..	19
B. Justice Consolidated Office Network (JCON).....	24
C. Joint Automated Booking System (JABS).....	30
D. Unified Financial Management System (UFMS).....	33
E. JCON-Secret and JCON-Top Secret (JCON-S/TS).....	38
<b>VII. Exhibit</b>	
A. Organizational Chart	
B. Summary of Requirements	
C. Program Increases/Offsets by Decision Unit	
D. Resources by DOJ Strategic Goal/Objective	
E. Justification for Base Adjustments	
F. Crosswalk of 2009 Availability	
G. Crosswalk of 2010 Availability	
H. Summary of Reimbursable Resources	
I. Detail of Permanent Positions by Category	
J. Financial Analysis of Program Changes	
K. Summary of Requirements by Grade	
L. Summary of Requirements by Object Class	
M. Status of Congressionally Requested Studies, Reports, and Evaluations	

## **I. Overview for Justice Information Sharing Technology (JIST)**

The FY 2011 JIST request includes \$179,785,000 and a total of 83 positions. JIST funds the Department's enterprise investments in Information Technology (IT). As a centralized fund under the control of the DOJ Chief Information Officer (CIO), it ensures that investments in IT systems, information sharing technology, enabling IT infrastructure enhancements, and cyber security are well planned and aligned with the Department's overall IT strategy and enterprise architecture. Given the level of staff dependence on the Department's IT environment (systems, networks, and data archives), CIO oversight is critical to the Department's legal, investigative, and administrative functions and the maintenance and improvement of DOJ staff productivity and effectiveness.

In FY 2011, the JIST appropriation will fund the Office of the CIO's performance of responsibilities under the Clinger-Cohen Act of 1996, the Department's response to OMB mandates, and eight programs that support the Overall Mission of the Department and contribute to the achievement of DOJ strategic goals. The nine JIST funded programs are:

- Investigation, law enforcement, litigation and intelligence
  - Joint Automated Booking System (JABS)
  - Law Enforcement Information Sharing Program (LEISP)
  - Litigation Case Management System (LCMS)
- Security and Secure Communications
  - Cyber Security Program (CSP)
  - Secret / Top Secret Communications (JCON S/TS)
  - Public Key Infrastructure/HSPD-12 (PKI)
- Critical Enabling IT Infrastructure
  - Justice Consolidated Office Network (JCON)
- Financial Management
  - Unified Financial Management System (UFMS)

### **Linkage to Strategic Goals**

JIST programs directly support the three Strategic Goals that are included in the Department's FY 2007-2012 Strategic Plan. These are:

- Strategic Goal 1: Prevent terrorism and promote the nation's security.
- Strategic Goal 2: Prevent crime, enforce federal laws, and represent the rights and interests of the American People.
- Strategic Goal 3: Ensure the fair and efficient administration of justice.

In addition to the above three Strategic Goals, DOJ recognizes "Strategic Goal 4: Enabling administration" as a fourth Strategic Goal. It allows and enables staff and other programs to pursue the other Strategic Goals in an effective and efficient manner. The JIST Program Description section links each program to the Strategic Goal supported.

## II. Summary of Program Changes

Item Name	Description				Page
		Pos	FTE	Dollars (\$000)	
LCMS	Deploy the LCMS to the Stage 2 Litigation Divisions. The deployment for Stage 2 Components and stand-alone LCMS services to Stage 3 Components will cover the 3-year period FY 2011 – FY 2013.	0	0	\$ 23,200	19
JCON	Refresh office automation systems for the 16 JCON supported components on a 4-year cycle and migrate components to the more secure and efficient JCONext service platform.	0	0	\$ 15,000	24
JABS	Upgrade JABS software modules, replace obsolete fingerprint livescan devices, and integrate JABS with new peripheral devices to maintain compatibility with the FBI's biometric and criminal history data repositories.	0	0	\$ 6,000	30
UFMS	Implement enhancements required for UFMS integration and implementation activities and Program Management Office staffing.	11	6	\$ 42,132	33
JCON S/TS	Upgrade and expand the communication infrastructure of data classified as Secret, Top Secret, and Sensitive Compartmented Information.	0	0	\$ 4,300	38

### III. Program Changes by Decision Unit to Strategic Goal

Item Name	Strategic Goal	Decision Unit	FTE	Dollars (\$000)	Number and Type of Positions	
					Position Series	No. of Positions in Series
LCMS	3	JIST	0	\$ 23,200		
JCON	Enabling/ Administrative	JIST	0	\$ 15,000		
JABS	2	JIST	0	\$ 6,000		
UFMS	Enabling/ Administrative	JIST	6	\$ 42,132	2210	11
JCON S/TS	1,2,3	JIST	0	\$ 4,300		

#### **IV. Appropriations Language and Analysis of Appropriations Language**

##### **Appropriations Language**

For necessary expenses for information sharing technology, including planning, development, deployment, and departmental direction, [\$88,285,000] \$179,785,000 to remain available until expended, *of which not less than \$42,132,000 is for the Unified Financial Management System.*

## V. Decision Unit Justification

### A. Justice Information Sharing Technology – (JIST)

<b>JIST - TOTAL</b>	<b>Perm. Pos.</b>	<b>FTE</b>	<b>Amount (\$000)</b>
2009 Enacted	71	71	80,000
2009 Supplementals			
2009 Enacted	71	71	80,000
2010 Enacted	72	72	88,285
Adjustments to Base and Technical Adjustments			868
2011 Current Services	72	72	89,153
2011 Program Increases	11	6	90,632
2011 Request	83	78	179,785
<b>Total Change 2010-2011</b>	<b>11</b>	<b>6</b>	<b>91,500</b>

<b>JIST – Information Technology Breakout</b>	<b>Perm. Pos.</b>	<b>FTE</b>	<b>Amount (\$000)</b>
2009 Enacted	71	71	80,000
2009 Supplementals			
2009 Enacted	71	71	80,000
2010 Enacted	72	72	88,285
Adjustments to Base and Technical Adjustments			868
2011 Current Services	72	72	89,153
2011 Program Increases	11	6	90,632
2011 Request	83	78	179,785
<b>Total Change 2010-2011</b>	<b>11</b>	<b>6</b>	<b>91,500</b>

#### 1. Program Description

##### Overview

JIST provides for the performance of Departmental responsibilities assigned to the CIO by the Clinger-Cohen Act of 1996, including the implementation of a capital planning and investment control process, the development and maintenance of an information technology architecture, the establishment of IT performance measures and IT security programs, and the development of strategies for improving information resources management. In addition to ensuring the CIO complies with the Clinger-Cohen Act and other applicable laws, rules, and regulations, the JIST appropriation funds specific IT programs, system development projects, enterprise-wide security infrastructure, and cyber security monitoring, to help provide a modern and secure IT environments to support the daily activities of the Department's agents, attorneys, analysts, and administrative staff. The following table presents an overview of JIST investments and programs and their relationship to the DOJ strategic goal:

Justice Information Sharing Technology													
Supported Programs													
		FY 2009 Enacted				FY 2010 Enacted				FY 2011 President's Budget			
Investments / Supported Programs	Strategic	POS	DME	O&M	Total	POS	DME	O&M	Total	POS	DME	O&M	Total
Investigation, law enforcement, litigation and intelligence													
Joint Automated Booking System (JABS)	2	7.0	-	9.0	9.0	7.0	-	9.6	9.6	7.0	-	19.7	19.7
Law Enforcement Information Sharing Program (LEISP)	1,2	3.0	2.3	1.7	4.0	3.0	2.8	1.5	4.3	3.0	3.5	2.0	5.5
Litigation Case Management System (LCMS)	3	3.0	16.9	-	16.9	3.0	-	-	-	3.0	23.2	-	23.2
IT Security and Secure Communications													
Cyber Security Program (CPS)													
IT Security	1,2,3	4.0	-	0.5	0.5	5.0	-	0.6	0.6	5.0	-	0.8	0.8
Trusted Internet Connection (TIC) / Security Infrastructure	1,2,3	-	-	-	-	-	15.4	-	15.4		15.3	-	15.3
Total - CSP		-	-	0.5	0.5	-	15.4	0.6	16.0	5.0	15.3	0.8	16.1
Secret /Top Secret Communications (JCON S/TS)	1,2,3	3.0	-	5.5	5.5	3.0		5.5	5.5	3.0	-	9.9	9.9
Public Key Infrastructure / HSPD-12 (PKI)	1,2,3	6.0	2.3	2.3	4.5	6.0	1.7	4.3	6.0	6.0	1.7	4.4	6.1
Critical Enabling IT Infrastructure													
Justice Consolidated Office Network (JCON)													
Secure office automation systems	4	3.5	9.4	11.4	20.8	3.5	6.5	12.0	18.5	3.5	31.5	12.0	43.5
Central Services	4	3.5	5.8	-	5.8	3.5	1.7	-	1.7	3.5	6.5	-	6.5
Total - JCON		7.0	15.2	11.4	26.6	7.0	8.2	12.0	20.2	7.0	38.0	12.0	50.0
Financial Management													
Unified Financial Management System (UFMS)		14.0	-	7.1	7.1	14.0	-	19.7	19.7	25.0	21.0	21.1	42.1
DOJ IT Management and Innovation													
OCIO - DOJ IT Management Functions	4	16.0	-	4.4	4.4	16.0	-	5.4	5.4	16.0	-	5.6	5.6
CTO - Technology Innovations	1,2	8.0	-	1.5	1.5	8.0	-	1.6	1.6	8.0	-	1.6	1.6
Total JIST		71.0	36.6	43.4	80.0	72.0	28.1	60.2	88.3	83.0	102.7	77.1	179.8

POS - Authorized Permanent Positions.



## **Joint Automated Booking System (JABS)**

JABS is a nationwide automated booking system for DOJ law enforcement agencies. It is the Department's "front end" to the FBI's Integrated Automated Fingerprint Identification System (IAFIS). Including booking stations maintained by DHS, JABS provides booking services to a total of 2,800 sites. Of those sites, JABS is responsible for the provisioning, maintenance and evolution of 1,100 workstations within the DOJ. JABS processes over 2 million transactions per year, accounting for nearly 85% of the Federal booking transactions submitted to IAFIS. JABS has reduced the time to identify an individual from several weeks for a paper fingerprint submission to about 30 minutes.

JABS operates and maintains a JABS data repository of biographic, biometric, charging and disposition information collected by the booking stations. Through OneDOJ, an information sharing exchange developed by the LEISP, JABS provides this information to counter terrorism and law enforcement fusion centers. This collection of 3 million booking records is especially noted for its extensive detail on suspects' scars, marks, and tattoos. This data has been cited by law enforcement as being especially useful in identifying persons when fingerprints are not available in data bases.

JABS is also charged with providing information interchange services that will eliminate the need to perform redundant bookings when prisoners are moved within DOJ. Major initiatives over the next several fiscal years include upgrading the data repository equipment, implementing data exchange capabilities, replacing the booking station biometrics collection equipment, and enhancing the operating systems to meet the new biometric collection and transaction required by various recent legislation including iris scans, DNA sample acquisition support, and palm prints.

## **Law Enforcement Information Sharing Program (LEISP)**

LEISP is a department-wide strategic approach for sharing data amongst DOJ components and between DOJ and other federal agencies and partners at the state, local and tribal level. It provides an overall collaborative framework and technological infrastructure for law enforcement information sharing. LEISP aims to reduce crime and to prevent terrorism by providing an overall framework and the technological means for the law enforcement community to share information quickly and effectively.

LEISP is an executive oversight program that provides the lynchpin for connecting several ongoing projects within key DOJ components, under a common set of goals and objectives. JIST supports the development and implementation of LEISP-related database application systems that enable state, local, and Federal law enforcement agencies nationwide to collect, share, and analyze law enforcement information on criminal activities and separately, in a more tightly controlled environment, to share and analyze sensitive intelligence data.

## **Litigation Case Management System (LCMS)**

The objective of the LCMS program is to acquire and implement a common litigation case management system for the US Attorneys and the seven DOJ litigating divisions. The program is developing a target architecture and infrastructure to effectively capture case related information once and to share the information within and between Department Components, partners, agencies, and the public. By establishing common data elements and applying automated tools to share information, the LCMS is expected to yield improvements in operational efficiencies across the U.S. Attorneys and the seven Litigation Divisions through greater information sharing. Attorneys, agents, and other staff will have easy and quick access to more electronically stored case information than ever before. The automated information sharing tools will be designed to eliminate duplicative data entry and time spent on retrieving and validating information not resident in the requestor's systems – this means legal staff will spend less time entering data and searching case files, and more time working on the case. LCMS will reduce operational costs, as well as to standardize reporting, to more effectively share information between the DOJ litigating divisions and DOJ executive leadership, Congress, OMB, and partner agencies. The program will also share information with other key DOJ systems including the FBI's SENTINEL for law enforcement

investigative case management and the Consolidated Debt Collection System (CDCS), further reducing the level of human effort required to share information.

The JIST account has funded \$55.6M to develop the LCMS for deployment to the U.S. Attorneys offices. The LCMS will be deployed to the initial Maine pilot site in early FY 2010, followed by a nationwide deployment to the remaining U.S. Attorney's offices.

### **Cyber Security Program (CSP)**

The Department has established two complementary programs – the Justice Security Operations Center (JSOC) and the Cyber Security Program (CSP) - to protect its IT environments (systems, networks, and sensitive data) from cyber attacks to ensure their availability for the Department's agents, attorneys, analysts, and administrative staff to continue their legal, investigative, and administrative functions. The JSOC is funded by the Department's Working Capital Fund. It proactively monitors (and maintains situational awareness) the Department's networks, investigates incidents, and develops signatures to block further intrusions. The CSP, funded by the JIST appropriation, is undertaking a multi-year program to implement DOJ enterprise-wide security architecture to secure networks and consolidate internet gateways.

The effectiveness of the JSOC to proactively defend against and respond to a cyber attack depends on establishing a limited number of Internet access points, Trusted Internet Connections (TIC), and an enterprise-wide security infrastructure. The CSP will establish the TIC and secure the Department's networks by:

- Modernizing intrusion detection systems (IDS) and firewalls across DOJ, including component networks,
- Providing common mandatory server/computers settings that are managed centrally to enable more timely and coordinated responses to security threats,
- Implementing a centrally-managed, departmental email system capable of hosting end-user emails accounts for the greatest number of components, and
- Segmenting message traffic by type to allow JSOC to customize data monitoring and apply specific countermeasures for each traffic type.

In addition to securing the Department's networks, CSP will support the JSOC by establishing a secure communications facility to support the exchange of information with USCERT and the Intelligence Community to enhance DOJ's ability to identify and respond to incidents caused by evolving cyber threats. This facility will allow JSOC to leverage the advance collection and analysis capabilities of USCERT and the Intelligence Community, use these capabilities to proactively secure the Department's systems and networks, and to work collaboratively on analysis and countermeasures for ongoing security incidents.

The Department's ability to achieve its strategic goals depends heavily on its ability to capture, process, manage, analyze, and share information. To meet mission investigative and information sharing requirements, DOJ's agents, attorneys, and analysts are increasingly reliant on connectivity to the Internet to enable collaboration with other DOJ components and multiple levels of government. This connectivity level increases the exposure of DOJ systems to disruption from cyber threats and attacks. The complementary JSOC and CSP programs directly supports the Department's Strategic Goals by providing DOJ with an effective security structure to counter current and emerging cyber threats and to ensure that our agents, attorneys, and analysts can continue using the Department's IT systems and networks to support their missions without significant interruption of service resulting from cyber attacks.

### **JCON-Secret and JCON-Top Secret (JCON-S/TS)**

The Department did not have a system for secure classified intra/inter-departmental data communications at the time of the September 11, 2001 terrorist attack. In response to the significant increase in classified mission needs after the 9-11 terrorist attack, the Attorney General directed that a secure communication system be implemented. JCON-S/TS networks were established in FY 2005 to provide an enterprise-wide, seamless

Information Technology (IT) infrastructure for electronically sharing, processing, and storing information classified at the Secret and Top Secret Levels. Currently, it provides secret and top secret/SCI service to all of the Department's components along with other Government Agencies.

JCON-S/TS networks are major enablers in allowing investigators, intelligence analysts, and attorneys at DOJ locations across the country and around the world to use and share classified case data. These networks use existing DOJ wide area networks, while connecting to other agencies via the worldwide backbone router networks (Secret Internet Protocol Routing Network and Joint Worldwide Intelligence Communication Systems) operated by the Department of Defense. Currently, there are over 1,000 JCON-S/TS workstations deployed, supporting over 3,000 users within the Continental United States and other U.S. Territories such as Alaska, Hawaii, Guam, and the U.S. Virgin Islands. Since inception, the JCON-S/TS have been a critical element of the Department's Continuity of Government and Continuity of Operations plans.

JIST funds the JCON-S/TS software and hardware at user and central data center sites and the JCON-S/TS Program Management Office responsible for planning, acquisition, and implementation of this software and hardware.

### **Public Key Infrastructure (PKI)**

The PKI program consolidates several security related initiatives by developing the enterprise architecture policies, best practices, and standards for HSPD-12 investment and IT improvements across DOJ. This program provides the planning, training, operational support, and oversight of the Personal Identification Verification card (PIVCard) deployment process for DOJ component employees and contractors.

The PIVCard is the center piece of the HSPD-12 solution being implemented government-wide. Standards set by National Institute of Standards and Technology (NIST) are the basis for satisfying identification and security requirements and for the use of a common PIVCard to achieve both logical and physical access to Federal-controlled facilities and information systems. The PIVCard contains logical elements including PKI certificates, digital photos, and fingerprint biometrics. The PIVCard and related processes will greatly enhance security, increase efficiency, reduce identity fraud, and protect personal privacy

The program serves as the DOJ's departmental issuer of PIVCards which is a mandatory element of the Department's compliance with government standards, and will allow cross-agency secure communications. The key values of the overall program are:

- Establish a single, authoritative authentication mechanism for DOJ which will expedite (single sign-on) and expand secure access to critical information,
- Enable identity authentication prior to accessing facilities and information systems,
- Create related infrastructure services at DOJ to provide for digital signatures, and end-to end encryption of sensitive law enforcement and terrorist related information, and
- Support information access and sharing by upgrading the IT infrastructure (Enterprise Directory, enterprise messaging, stovepipe component infrastructures and enterprise networking) to support secure communications especially between persons from different organizations.

### **Justice Consolidated Office Network (JCON)**

The JCON program provides architecture guidance and funding to build reliable, secure office automation systems and component infrastructure (desktops, laptops, servers, local area networks and data storage) upon which 16 DOJ litigation, management, and law enforcement components operate their mission-critical applications. By providing for the maintenance of the JCON Standard Architecture, centralized acquisition management, a standardized system development and implementation methodology, configuration management, and financing for new system deployments, JCON promotes interoperability and information sharing among

DOJ components and their business partners, *e.g.*, courts, other components, and federal agencies. The key elements of the DOJ JCON strategy to maintain secure office automation systems are:

- Establish a standard DOJ workstation, and
- Establish a predictable technology refresh cycle to ensure that all JCON components have current, secure, and compatible messaging technologies that enable collaboration within the Department, as well as with other law enforcement agencies.

Increasingly, DOJ systems and networks are required to meet stringent security and operating parameters, including additional record management requirements, encryption and data auditing, scanning requirements, new common DOJ applications, and OMB mandates. The JCON Program is critical for the Department to address and fund the requirements to support the current more stringent security and operating parameters.

Since 2005, JCON has pursued a course to standardize requirements by developing centralized enterprise-class systems to support multiple components with common office automation needs. This includes Enterprise Directory systems, Enterprise Email and messaging platform, Enterprise monitoring, management and help desk, Enterprise-wide desktop imaging, and others. Implementation of this suite of centralized systems will enhance the capability of the Department to develop an effective and less expensive cyber defense program and will yield a more cost effective platform for the delivery of key office automation services.

### **Unified Financial Management System (UFMS)**

UFMS is an enterprise-wide Financial Management System that will enable DOJ to streamline and standardize financial business processes across all components, providing secure, accurate, timely, and useful financial and procurement data to program managers across the Department, and will produce component and department-level financial statements. The UFMS will facilitate the DOJ compliance with the CFO Act by improving procurement and financial management performance and aid department components in establishing and maintaining strong internal controls, complying with accounting standards, and ensuring system security.

### **OCIO – DOJ IT Management Functions**

JIST funds the Policy & Planning Staff (PPS) that supports CIO management in complying with the Clinger-Cohen Act and other applicable laws, rules, and regulations for federal information resource management. PPS develops, implements, and oversees an integrated approach for effectively and efficiently planning and managing DOJ's information technology resources. PPS performs these responsibilities by managing of the following Department-wide processes: CIO Council, Department Investment Review Board (DIRB), IT Strategic Planning, IT Audits, Enterprise Architecture, IT Governance, IT Investment and Paperwork Reduction Act.

PPS includes groups responsible for enterprise architecture (EA) and infrastructure architecture (IA). EA monitors and ensures compliance with OMB and GAO enterprise architecture requirements, advises the CIO on strategic priorities, and works to drive these priorities. To achieve these objectives, the chief enterprise architect undertakes/monitors IT strategic planning, documents the Department-wide EA, performs EA governance across the department, supports investment reviews (DIRB and ITIM), and develops detail architectures for the Department-wide segments, such as information sharing, in collaboration with key stakeholders from across the Department.

IA is the tactical side of EA. It is responsible for the reviewing and consolidating the infrastructure OMB 300 submissions, planning OMB infrastructure initiatives such as cloud computing, performing assessments of enterprise infrastructure development and maintenance, providing IA consultation with PMOs, and assessing IA plans throughout OCIO and the Department. To execute these responsibilities, IA conducts Department level reviews and analyses, validates technical approaches with respect to architecture, assesses development and

deployment approaches, performs other analysis that evaluates the effectiveness of infrastructure planning and deployment, makes recommendations for improvement of the DOJ infrastructure performance and for cost efficiency, and prepares technical analysis and reports.

### **Chief Technology Office – Technology Innovations**

The CTO identifies and implements innovative new technologies that can result in cost effective IT solutions of the Department. Currently, the CTO is working on the following:

- **Data Standards:** Developing and implementing standard information structures and exchange standards that enable information exchange between federal, state, local, and tribal enforcement and intelligence organizations. Identity & Access Management – Implementing a secure, scalable means of authenticating users.
- **Identity & Access Management:** Developing a cost-effective approach for providing a scalable identity authentication service across the DOJ enterprise.
- **Information Sharing Infrastructure:** Developing tools and techniques that enable or facilitate information sharing with DOJ's federal, state, and local partners.
- **Information Fusion:** Collaboratively building best-of-breed prototypes tools for Search and Correlation and sharing lessons learned with major DOJ programs. Geospatial Information Services (GIS) – Develop an enterprise GIS Infrastructure Services to greatly reduce the cost and effort to implement GIS applications and initiatives across DOJ.
- **Geospatial Information Services (GIS):** Establishing baseline GIS services and training to jumpstart mission-specific GIS projects.

PERFORMANCE AND RESOURCES TABLE											
Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)											
DOJ Strategic Goal/Objective: Overall Mission Support Thru IT / Protecting America from the threat of terrorism											
WORKLOAD/ RESOURCES		Final Target		Actual		Projected		Changes		Requested (Total)	
		FY 2009		FY 2009		FY 2010 Enacted		Current Services Adjustments and FY 2011 Program Change		FY 2011 Request	
Workload											
Total Costs and FTE (reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)		FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		71	80,000 [54,980]	71	80,000 [71,245]	72	88,285 [158,969]	6	91,500 [ -66,531 ]	78.0	179,785 [92,438]
TYPE/ STRATEGIC OBJECTIVE	PERFORMANCE	FY 2009		FY 2009		FY 2010 Enacted		Current Services Adjustments and FY 2011 Program Change		FY 2011 Request	
Program Activity		FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
		71	80,000 [54,980]	71	80,000 [71,245]	72	88,285 [158,969]	6	91,500 [ -66,531 ]	78	179,785 [92,438]
Performance Measure	Percentage of offenders booked through JABS		99%		99%		99%		-		99%
Performance Measure	Percentage of total JCON workstations deployed in the fiscal year (non-cumulative)		100%		73%		100%		-		100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations		99%		99%		99%		-		99%
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations		99%		99%		99%		-		99%
Performance Measure	Ensure IT systems are certified and accredited		100%		100%		100%		-		100%
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms		74%		76%		75%		-		75%

PERFORMANCE MEASURE TABLE											
Decision Unit: JMD/OCIO/Justice Information Sharing Technology (JIST)											
Performance Report and Performance Plan Targets		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009		FY 2010	FY 2011
		Actual	Actual	Actual	Actual	Actual	Actual	Target	Actual	Target	Target
Performance Measure	Percentage of offenders booked through JABS	N/A	N/A	95%	97%	99%	99%	99%	99%	99%	99%
Performance Measure	Percentage of total JCON workstations deployed in the fiscal year (non-cumulative)	N/A	N/A	N/A	45%	0%	15%	100%	73%	100%	100%
Performance Measure	Maintain mainframe enterprise system availability for client organizations	N/A	N/A	N/A	N/A	100%	100%	99%	99%	99%	99%
Performance Measure	Maintain JMD/SMO JCON system availability for client organizations	N/A	N/A	100%	99%	100%	100%	99%	99%	99%	99%
Performance Measure	Ensure IT systems are certified and accredited	N/A	N/A	91%	92%	100%	100%	100%	100%	100%	100%
Performance Measure	Ensure IT help desk calls are answered and resolved within service level agreement terms	N/A	N/A	N/A	N/A	87%	78%	74%	76%	75%	75%

N/A = Data Unavailable

### 3. Performance, Resources, and Strategies

#### a. Performance Plan and Report for Outcomes

JIST consolidates certain IT resources so that the DOJ CIO can more effectively coordinate DOJ IT investments and directly finance certain infrastructure improvements.

*Oversight of these resources and key programs* is critical to their success and ensuring outcomes that support the Department's mission.

In FY 2006, the Department established a Department IT Investment Review Board (DIRB). Members of the DIRB are composed of the Department of Justice (DOJ) executive officers, augmented by non-voting DOJ representatives and component members. The Deputy Attorney General (DAG) chairs the board and the DOJ CIO serves as vice chair. The DIRB is composed primarily of members with IT subject matter and financial management expertise, thereby providing complementary perspectives on the best use of resources to improve the management of IT investments of the Department.

The DIRB provides the highest level of investment oversight as part of the Department's overall IT investment management process. The Department's IT investments are vetted annually through the budget submission process, in conjunction with each component's Information Technology Investment Management (ITIM) process. Of the hundreds of projects that are funded annually across the Department, approximately a dozen are selected each year for DIRB review based on the size of their budget and/or their strategic importance to the Department's mission. The DIRB's principal functions in fulfilling its decision-making responsibilities are to:

- Ensure compliance with the Clinger-Cohen Act and all other applicable laws, rules, and regulations regarding information resources management,
- Monitor the Department's most important IT investments throughout their project lifecycle to ensure goals are met and the expected returns on investment are achieved,
- Ensure each project under review has established effective budget, schedule, operational, performance, and security metrics that support the achievement of key project milestones,
- Review the recommendations and issues raised by the components' IT investment management process,
- Review annually each component's IT investment portfolio, including business cases for new investments, to enable informed departmental IT portfolio decisions,
- Develop and implement decision-making processes that are consistent with the purposes of the DIRB, and with applicable Congressional and OMB guidelines for selecting, monitoring, and evaluating information system investments (these processes shall be designed to ensure that the DIRB's decisions are consistent, valid, and actionable, support the Department's business needs and processes, align with the Department's strategic goals and objectives, comply with enterprise architecture, and consider the delivery of a modernized IT infrastructure and efficient, effective services as a driving goal), and
- Establish a communication plan that conveys DIRB actions and progress against the Department's identified processes and goals.

In addition to the DIRB, the Department has established an IT Dashboard that allows management to review various aspects of major initiatives across the Department. The Dashboard is considered another oversight tool since all projects cannot be reviewed by the DIRB. The dashboard includes Earned Value Management System (EVMS) reporting to ensure projects are evaluated against acceptable variances for scope, schedule, and costs. Risk analysis and project funding information are also available in this tool. This allows the Department's CIO and senior management team to have timely access to project information via the web.



## **b. Strategies to Accomplish Outcomes**

Specific mission critical IT infrastructure investments are designed, engineered and deployed with JIST resources.

- The complementary JSOC and CSP programs provides for the implementation and maintenance of an enterprise-wide security architecture to reduce the number of Internet access points and deploy a cyber attack defense-in-depth strategy to lessen the effectiveness and impact of external cyber attacks with the capability to conduct end-to-end monitoring of data traffic flows and to take defensive actions when and where necessary.
- LEISP creates the core law enforcement information sharing services that will allow information to be routinely exchanged between agencies and their systems. Its objectives are to:
  - Integrate several existing or newly initiated DOJ funded information sharing systems.
  - Direct the integration and support the timely completion of ongoing projects by infusing project coordination guidance, technology direction, and project oversight from the Office of the CIO.
  - Provide access to other federal, state, and local agency communications infrastructure to exchange law enforcement information. This will be achieved by connecting (or enhancing existing connections) between DOJ networks (JUTNET, CJIS WAN, LEO) and the networks of other federal partners such as the Department of Homeland Security (DHS), as well as selected state/local networks such as the National Law Enforcement Telecommunications System (NLETS) and the Regional Information Sharing System (RISS).
- Develop and implement an electronic authentication system to allow authorized users from other federal, tribal, state, and local law enforcement agencies to access DOJ information from the core LEISP services. The electronic authentication system is necessary to identify individuals who are accessing DOJ through the core LEISP services with a high level of confidence. Positive electronic identification that includes personally identifiable information ensures that data is accessed only by authorized agents/officers, and is necessary to allow DOJ to track and audit DOJ law enforcement data access, a requirement of the Privacy Act. The LEISP intends to leverage the DOJ PKI program to achieve this objective.
- Connect select data sources from other federal law enforcement agencies (e.g., DHS) to the core LEISP services. To achieve this objective requires the OCIO to develop and implement one or more data source adapters similar to those discussed above for DOJ component data sources.
- The LCMS is an initiative to use centrally managed fund and corporately controlled planning, engineering, acquisition and deployment resources to improve operational efficiency through greater case related information sharing. By implementing common data elements and applying automated tools to share information, agents, attorneys, and other staff will have access to more information, more quickly and easily. Further, the implementation of common standards for identifying and processing litigation cases will enable the Attorney General to manage and deploy the Department's legal staff and caseload more effectively
- The JCON Program is a mature infrastructure program that provides a reliable and robust common office automation platform upon which 16 of the DOJ litigating, management, and law enforcement components operate their mission-critical applications. JCON centrally funds and manages the planning, acquisition, and implementation of a commercial-off-the-shelf (COTS) product-based office automation solution for participating components across the Department.
- JABS is a nationwide automated booking system for DOJ law enforcement agencies and serves as the information sharing system that eliminated redundant successive bookings, and established a federal offender tracking system by enabling agencies to share and exchange booking information. It is the Department's "front end" to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) which provides an automated process for the collection and

transmission of fingerprint, photographic, and biographical data. JABS enables agencies to share and exchange booking information and maintain federal offender tracking capability.

- The PKI program was started by consolidating several security related initiatives. The program develops the enterprise architecture policies, best practices and standards for HSPD-12 investment, and IT improvements across DOJ and provides planning, training, operational support and oversight of the Personal Identification Verification card (PIVCard) deployment process for DOJ component employees and contractors. The PIVCard contains logical elements including PKI certificates, digital photos, and fingerprint biometrics and will be used by government employees and contractors for achieving both logical and physical access to Federal controlled facilities and information systems.

### **c. Results of Program Assessment**

JIST has not been selected for a Program Assessment review.

## VI. Program Increase

<b>Item Name:</b>	<b>Litigation Case Management System (LCMS)</b>
<b>Budget Decision Units:</b>	JIST
<b>Strategic Goal(s) &amp; Objective:</b>	Ensure the fair and efficient administration of justice.
<b>Organizational Program:</b>	JIST
<b>Component Ranking of Item:</b>	1 of 5

**Program Increase:** Positions 0 FTE 0 Dollars \$23,200,000

### **Description of Item**

The FY 2010 Consolidated Appropriation Act (H.R. 3288) states that a reprogramming of funds of the LCMS program will be considered once the Department has completed all of the Inspector General's LCMS recommendation and submitted a report to the House and Senate Committees on Appropriations detailing the steps taken to contain costs and schedule overruns. Since the required LCMS report has been submitted to and approved by the Office of Management and Budget, the Department is requesting a \$32.9 million reprogramming of WCF UBT funding for the continuing development of the LCMS. The \$32.9 million reprogramming will allow the program to complete the deployment of LCMS across the EOUSA and begin the planning and design for the LCMS Stage 2 Litigation Division Group (CIV, CRT, and ENRD). These funds will be utilized over a two-year period.

LCMS is requesting a FY 2011 program increase of \$23.2 million including restoration of \$14.2M base, recurred for FY 2012 and FY 2013, to allow the LCMS to be implemented for EOUSA in FY 2011 and deployed to the Stage 2 Litigation Divisions over the period FY 2011 – FY 2013. Including the \$8.4 million carryover funding from the FY 2010 reprogramming, the total budget available to LCMS in FY 2011 is \$31.6 million.

These resources will fund the completion to become the common case management solution across the U.S. Attorneys and the seven Litigation Divisions. Without the funding increase, the LCMS will be implemented as a U.S. Attorneys' system only and the Department will not realize the primary program benefit of a common case management solution that delivers timely and accurate management reporting and decision support information across components.

The objective of the LCMS Program is to acquire and implement a common litigation case management system for the U.S. Attorneys and the seven Litigating Divisions. LCMS will allow the Department to reduce operational costs through effective single-point capture of case information and appropriately sharing the information between the U.S. Attorneys and the seven Litigating Divisions (Antitrust Division, Criminal Division, Civil Rights Division, Civil Division, Environment and Natural Resources Division, National Security Division, and Tax Division) and with DOJ executive leadership, Congress, OMB, and partner agencies. The LCMS will also share information with other key DOJ systems including the FBI's Sentinel for law investigative case management and the Consolidated Debt Collection System (CDCS).

The LCMS Program is planned to be implemented in three stages:

- i. Stage 1 - Develop, test, and deploy LCMS to the 94 U.S. Attorneys' Offices with the LCMS Justice Data Center hosting environments.
- ii. Stage 2 – Requirements definition, develop, and deploy to CIV, CRT, and ENRD
- iii. Stage 3 – Requirements definition, develop, and deploy to CRM/NSD, TAX, and ATR. This stage may leverage the existing Case Management applications for the groups, while integrating the data with LCMS for cross-component sharing and common DOJ reporting.

The LCMS team is working closely with EOUSA to deploy a pilot to USA-Maine in early calendar year 2010. The pilot will fully support district operations and will serve as a Field User Acceptance test for the application.

The LCMS Program Management team and EOUSA will then evaluate the results from this operational pilot and finalize the full deployment plans across all of the U.S. Attorney's Offices. The requested FY 2011 increase will fund the detailed planning and design for LCMS Stage 2 and 3, including requirements definition for all seven Litigation Divisions and the start of the deployment to the Stage 2 Litigation Division group (CIV, CRT and ENRD). This increase specifically positions ENRD as the next Component for Stage 2 deployment followed by CRT and CIV. The rollout of LCMS to the seven Litigation Divisions (Stage 2 and 3 groups) will occur during the three-year period FY 2011 – FY 2013, recognizing that the Stage 3 groups may leverage their existing case management applications during this timeframe.

## **Justification**

The DOJ's current case management environment does not support efficient, automated information sharing, or streamlined reporting and decision support capabilities. The U.S. Attorneys and Litigating Divisions are highly decentralized, with case information entered and stored in numerous, disconnected legacy systems. When case file information needs to be shared between a litigating division and a U.S. Attorneys' Office, copies of the paper files are made and are sent via mail or courier. A similar process occurs when law enforcement or investigation information is shared between an outside agency and the U.S. Attorneys.

When case information is received from another DOJ component, the US Attorneys create another independent case file, and re-enter case data into their own case management system. Once a U.S. Attorney takes the lead on the case, the originating component or law enforcement agency no longer has the ability to monitor case status, or access updated case information. The loss of access to monitor and update case information results in the originating component or law enforcement agency tracking issues as separate instances with multiple results, instead of all of the related data being tracked and maintained as a single case. Executive decision support information and cross-DOJ performance data is also very difficult to obtain due to multiple, disparate data sources.

The case management system feasibility study, conducted in FY 2005, identified several factors that provide immediate opportunities for a DOJ common litigation case management solution:

- Several litigating components have immediate case management system needs, including three components using LawPack, a system that has not been supported by the vendor since December, 2004. (CIV, CRT, ENRD).
- Five of the litigating components were pursuing their own independent solutions; thus, there are immediate opportunities to reduce overlapping case management investments.
- EOUSA's Enterprise Case Management System (ECMS) Program was being re-assessed, presenting an opportunity for the common solutions initiative to partner with EOUSA to develop common solutions for the DOJ litigation community as a whole instead of just for the U.S. Attorneys.

With three components using a system sunset by the vendor, several components with similar needs pursuing solutions independently, and EOUSA re-assessing the ECMS Program, Department management decided that the best approach would be to establish the LCMS Program to pursue a common solution across Litigating Components.

The objective of the LCMS Program is to acquire and implement a litigation case management system for the U.S. Attorneys and the seven Litigation Divisions. By the end of FY 2010, the LCMS system will be developed and tested, and deployment will begin to the U.S. Attorney's Offices. However, the continuation of the deployment of LCMS to the seven Litigation Divisions cannot proceed without a JIST funding increase.

Although Department Management approved the LCMS Program, the Program has not been supported by a dedicated base funding allocation. Since the JIST inception in FY 2006, JIST resources have been used to fund for the development and deployment of the LCMS to the U.S. Attorneys came from JIST funding available from

its inception in FY 2006. JIST increases were requested for FY 2007, FY 2008, FY 2009 and FY 2010 to provide a base funding for the program; however, none of these requests were approved. Therefore, the requested FY 2011 increase is necessary to continue deployment of the LCMS as the Department's common case management solution. Without the increase or other funding resources, the LCMS Program will essentially stop after the U.S. Attorneys' deployment.

The FY 2011 increase of \$23.2M should be recurring for FY 2012 and FY 2013 to fund the three-year LCMS deployment to the Stage 2 Litigation Divisions. In addition to the deployment to the Stage 2 Components, the LCMS program will deploy standalone LCMS services to Stage 3 Components during this timeframe. The specific services need to be finalized for each Component, but potential examples include Common Reporting, PACER integration, Document Management, and Advanced Reporting. The total funding required for the three-year rollout for Stage 2 and for the Stage 3 services is \$69.6M. Each office will sustain the costs for maintaining LCMS once it is deployed and operational. This will help ensure JIST funding for LCMS supports development and implementation of new technology.

In the May-August 2009 timeframe, the LCMS team conducted a series of executive meetings with DOJ leadership, including the Deputy Attorney General (DAG), the Associated Attorney General (ASG) and several staff members from their teams. As part of these meetings, these leaders have reconfirmed their executive sponsorship of LCMS and the goals of an enterprise case management solution. In particular, DOJ leadership recognizes the strong business value of an integrated solution that supports the cross-sharing of information, case management standardization across litigating components, real-time management reporting across components, and a centralized infrastructure for the integration of new enhancements, such as integration with the PACER court systems. These business results are contingent upon this incremental funding request.

### **Impact of Performance**

A common solutions approach leveraging common case management systems yields operational efficiencies resulting in enhanced support of the Department's mission of defending and protecting the interest of the U.S. Government by vigorously enforcing environmental, civil, tax, antitrust and bankruptcy laws. The approach also yields long-term cost savings benefits through the reduction of redundant legacy investments.

Improved operational efficiency will be achieved through greater information sharing. By implementing common data elements and applying automated tools to share information, law enforcement agents, attorneys, and other staff will have easy and quick access to more information. The automated information sharing tools will eliminate time spent on retrieving and validating information not resident in the requestor's systems, and duplicative data entry. The result will lead to more efficient litigation activities and more effective litigation results.

The LCMS Program is an essential investment under the OMB Lines of Business Program, and will provide benefits to other federal agencies. In support of the objectives of the Case Management Line of Business, the LCMS Program is developing a target architecture and infrastructure for sharing case related information within and between DOJ components, partner agencies, and the public, by developing a case management architecture that will effectively capture information once and make it available to all authorized users.

The LCMS Program will develop re-usable standards and building blocks (i.e., target architecture) and will create a model that can be used at other agencies to develop litigation case management solutions. These standards and architecture products will ensure greater case management information sharing and compatibility across agencies.

Joint procurement of solutions will present opportunities to save through economies of scale. By procuring solutions for a larger user base, cost per user will decrease. Additionally, components using the same systems will be able to leverage each other's expertise and system support resources. Common solutions, in conjunction with data standards, also set the stage for the second category of benefits, operational efficiency improvements.

In the May-August 2009 timeframe, the LCMS team conducted a series of executive meetings with DOJ leadership, including the Deputy Attorney General (DAG), the Associate Attorney General (ASG), several staff members from their teams, and the Executive Officers of all of the Litigating Components. During these meetings, the following benefits were emphasized as the key business drivers of LCMS:

- Improved interoperability and consistency across Litigating Components
- Adherence to standards compliance, which is a consistent recommendation from the IG and GAO and is important for any litigation information shared externally
- Efficient & timely reporting software and tools with a single data source with improved quality (“point & click” access)
- Cross-Department information for all areas of Case Management, including case types, appeals, win/loss, workload metrics, etc...
- Automated/expedited referral process for case transfers
- Improved visibility across Components for shared work
- Economies of scale and reduction of duplicative investments
- Increased Operational Efficiencies with platform for introduction of new capabilities (e.g., PACER, document management, etc...)
- Streamlined FOIA requests and improved consistency of FOIA business rules

Executive management also recognizes that the Stage 2 Components have an urgent need for a new solution, and those needs will not be addressed without this funding request. The case management system currently used by these Divisions are antiquated, difficult to maintain, and beginning to experience degradation in services. Ultimately, the capacity of these Divisions to meet their expanding operational missions including the increase in sharing cases across will be seriously diminished without this funding request and the LCMS system.

## Funding - LCMS

### Base Funding

FY 2009 Enacted				FY 2010 Enacted				FY 2011 Current Services			
Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)
3		3	\$16,868	3		3	0	3		3	0

### Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Not Applicable				
Total Personnel				

### Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Total Non-Personnel	\$23,200	1	\$23,200	\$0

### Grand Total

	Pos	Agt/Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)
Current Services	3		3	\$[548]	\$[13,652]	\$[14,200]
Increases				\$548	\$22,652	\$23,200
Grand Total	3		3	\$548	\$22,452	\$23,200

## VI. Program Increase

<b>Item Name:</b>	<b>Justice Consolidated Office Network (JCON)</b>
<b>Budget Decision Units:</b>	JIST
<b>Strategic Goal &amp; Objective:</b>	Enabling/Administration – Supports Goals 1-4
<b>Organizational Program:</b>	JIST
<b>Component Ranking of Item:</b>	2 of 5

**Program Increase:** Positions 0 FTE 0 Dollars \$15,000,000

### **Description of Item:**

This FY 2011 increase of \$15,000, recurred as an increase to the JIST base appropriation, will allow the Justice Consolidated Office Network (JCON) to fund:

- The refresh of workstations and related equipment for its 16 DOJ litigation, management, and law enforcement components;
- The migration of components to JCONext consolidated services platform ; and
- The operation of the basic JCONext consolidated services platform.

JCONext is the successor to the JCON IIA architecture currently used by 15 JCON-supported components. It will provide a more secure and efficient operating environment and should reduce DOJ-wide cost by centralizing messaging<sup>1</sup>, directory services<sup>2</sup>, collaboration services<sup>3</sup>, other utilities services<sup>4</sup> and storage services, as well as by centralizing operations of key common basic services (e.g. backup, virus scanning, firewalls, patching, etc.).

### **Justification:**

The JCON Program provides architecture guidance and funding to build reliable, secure office automation systems and component infrastructure (desktops, laptops, servers, local area networks, and data storage) for 16 DOJ litigation, management, and law enforcement components to operate their mission-critical applications and allow them to communicate with one another. JCON promotes interoperability and information sharing among DOJ components and their business partners, *e.g.*, courts, other components, and federal agencies through its maintenance of the JCON Standard Architecture, centralized acquisition management, a standardized system development and implementation methodology, configuration management, and financing for new system deployments. The 16 JCON components are as follows:

---

<sup>1</sup> Messaging services include Email accounts, message archiving, Blackberry Enterprise services and search support.

<sup>2</sup> Directory services include user accounts, computer accounts, server accounts and GPOs.

<sup>3</sup> Collaboration services include basic SharePoint access and MySite with limited storage per user.

<sup>4</sup> Utility services include antivirus downloads, key management services, monitoring, logging, security scanning, and backups.



<b>Component</b>	<b>Year Joined JCON</b>	<b>Users</b>
Antitrust Division (ATR)	Inception	1,000
Bureau of Prisons (BOP) <sup>5</sup>	2003	
Civil Division (CIV)	Inception	1,750
Civil Rights Division (CRT)	Inception	900
Community Relations Services (CRS)	2001	80
Criminal Division (CRM)	Inception	1,300
Environment and Natural Resources Division (ENRD)	Inception	850
Executive Offices for Immigration Review (EOIR)	2001	2,000
Executive Office for U.S. Attorneys (EOUSA)	Inception	16,000
Justice Management Division (JMD)	Inception	2,200
Office of Justice Programs (OJP)	Inception	1,200
Tax Division (TAX)	Inception	600
U.S. Marshals Service (USMS)	2002	6,500
United States National Central Bureau of INTERPOL (USNCB)	2004	150
U.S. Parole Commission (USPC)	2004	100
U.S. Trustees Program (UST)	2001	1,200
Total		35,830

### ***JCON Background***

The JCON program was initiated in 1996 to replace or substantially upgrade the office automation systems used by the Department's senior management, litigating, and related components. The Deputy Attorney General at that time determined it was in the Department's best interest for components to acquire funding for replacement systems under one consolidated program rather than each component acquiring funding for its systems independently. The primary goals set for JCON were to:

- Create a reliable, secure office automation system architecture which allows attorneys, law enforcement officials, and managers, the immediate ability to exchange all electronic data within and between components;
- Comply with the Attorney General's general policy of standardizing the legal and law enforcement tools used throughout the Department; and
- Obtain implementation, operation, and maintenance cost efficiencies.

These goals continue to be applicable to today's JCON. The need to meet a wide variety of security and compliance goals mandated by OMB in past years has driven additional consolidation and standardization and led much of the recent evolution of the JCON architecture. To achieve these goals, JCON has been and continues to be organized to conduct the following primary activities:

- Program Management Office – Program technical leadership, planning, coordination, management, facilitation activities, and contract administration;
- Component support – Direct component engineering support to maintain the JCON architecture, migrate to the next generation platform, when available, and operate the Common Office Automation Resources (COAR)<sup>6</sup> environment used to exchange emails between components;

<sup>5</sup> BOP received a \$6.8 M allocation from JCON in 2003. Subsequent to 2003, BOP has not received any additional JCON support.

<sup>6</sup> The COAR domain is a group of servers acting as the central hub for exchanging email between component-managed and JCON-managed domains, and outside of the JCON community. Over time, COAR has become expensive to run and no longer provides the benefits expected from a "centralized" system.

- Central services – Design and promulgate standard architecture and design and implement central infrastructure to ensure that the JCON components meet current security and operating parameters; and
- Component equipment – Purchase and install desktops, laptops and office-automation servers at component sites.

Central services activities have driven the evolution of JCON to effectively respond to technological changes and increasing security risks, while promoting interoperability and information sharing. In 1998, JCON initiated the JCON II architecture, Windows NT 4.0 with Exchange 5.5, to replace the existing JCON. To capture the benefits of technological changes and to ensure that JCON II continued as a viable platform, it was evolved into JCON IIA, Windows 2000 and Exchange 2000 Environment, that started to be deployed in 2002.

In recognition of the need to centralize office automation functions to reduce long-term costs, improve network security, and enhance user experience, in FY 2006, the JCON PMO began to design and plan the implementation of JCONext infrastructure as a successor to the JCON IIA platform. JCONext is a set of applications and infrastructure designed to centrally provide the next generation of directory, messaging, collaboration, utility services, and storage services. Earlier JCON designs focused exclusively on system design and implementation, and did not prescribe operational methods or include any actual system operation. Each component implemented JCON-funded systems independently and operated them separately, albeit based upon a similar architecture to other JCON systems across DOJ. JCONext contains a strong operational component, actually performing much of the basic operational duties of the centralized services on behalf of the component customer. As a result, JCON components electing to migrate to JCONext will be able to shut-off their E-mail systems and stop performing some common maintenance functions since these services will be provided centrally.

### ***JCON Funding***

The Legal Activities Office Automation (LAOA) direct appropriations account and Working Capital Fund (WCF) reprogrammings<sup>7</sup> funded JCON from inception through FY2005. In FY 2006, JCON was consolidated into the Justice Information System Technology (JIST) account along with the JABS, LEISP, JCON-S/TS, LCMS, PKI and UFMS programs.

The JCON funding under JIST has not kept up with requirements to operate and maintain the program, provide central services, and fund a 4-year component equipment refresh cycle. Since its consolidation with JIST, JCON's annual funding has declined as shown in the following table:

Fiscal Year		JIST Allocation (\$000,000)
FY 2006	Actual	\$34.9
FY 2007	Actual	\$49.4
FY 2008	Actual	\$33.5
FY 2009	Actual	\$26.6
FY 2010	Planned	\$20.2
Average FY 2006 - FY 2010		\$32.9

<sup>7</sup> LAOA received \$130 M from the WCF during the period FY 2001- FY 2003.

The average FY 2006-2010 JIST funding of \$32.9M is \$16.5M less than the average FY 2001-2005 LAOA/WCF funding of \$49.4M. The decline in the JIST JCON allocation is primarily caused by a \$15.5M Base reduction in JIST FY 2008 enacted (from \$100.5M FY 2007 Base to and \$85.0M FY 2008M base) and a further \$5.0M base reduction in the FY 2009 enacted. Since the JCON allocation decline is presented in nominal dollars, the real impact is much greater after adjusting for inflation during the 5-year period shown in the table.

JCON funded \$9.4M for component equipment refresh in FY 2009 and is forecast to fund only \$6.5M in FY 2010. This level of annual component equipment refresh (about \$8.0M) is not sufficient to maintain a 4-year equipment refresh cycle.

### ***JCON Component Equipment Support Requirement***

JCON, in conjunction with its components, has developed a forecast of component equipment support requirements based on the number and location of users, the cost of a standard office automation equipment set, and the component cost to migrate to JCONext. A component may elect to acquire and install other items (exchange servers, domain controllers, extensive routing networks, printers, SANs/NAS and other storage) or to upgrade the standard workstation; however, the component will be responsible for using its appropriation to pay the increased cost. The standard office automation set includes the following:

- Workstations (at BPA prices per person),
- Local office access switches (one port per person plus small additional for office-wide routers).
- Local office file, print servers (with moderate office automation file storage), and
- Installation services for these items.

The JCON PMO, working with its component, has determined that the FY 2011 JCON JIST allocation need to be about \$50.0M to meet the equipment refresh requirements of components scheduled for refresh in FY 2011 and to migrate those components to the JCONext consolidated service platform. Even with a planned significant increase in the JCON base in FY 2011, JCON needs a \$15.0M increase to meet its operational needs, while funding component equipment refresh. For JCON to maintain a 4-year equipment refresh cycle and to support components migrating to JCONext, the \$15.0M increase should be recurred as a JCON base increase. JIST is exploring how resources to maintain JCONext operations can be shared by the components who are actually using the system. This will help ensure JIST resources are targeted towards cost-effective modernization of JCON in support of the Department's emerging needs.

### **Impact on Performance**

The performance of DOJ components within the JCON system umbrella has been impacted positively by the acquisition and implementation guidance of the JCON PMO. Department-wide, DOJ has benefited from the standardization of office automation systems and the adoption of collaborative management practices. The JCONext evolution of the JCON architecture builds common operations and maintenance functions into the service offering, as well as introducing key concepts for cost management and security control as required by mandate and good practice. Examples of the specific performance achievements of the JCON program follow:

- Without JCON's centralized technical leadership and management, the 16 participating litigating, management, and law enforcement components would have to design, develop, and implement their own, separate office automation infrastructures to carry out their respective missions-related and business processes. These duplicative efforts would result in:
  - Increased costs due to economies of scale not being realized during the procurement of hardware, software, and contractor services;
  - No knowledge transfer and lessons learned; and
  - The inability to acquire consolidated technical support.

- Use of a Standard Architecture ensures interoperability and information sharing between components. Without this architecture, the resulting disparate systems would make it extremely difficult for components to share the information required to create electronic case files, briefs, and other legal documents necessary for prosecution. This is due to the fact that multiple operating systems and messaging platforms deployed within these components would not interoperate easily. The JCON architecture is robust enough to host component administrative and management applications and possesses the flexibility to provide access to all required external systems. The JCON architecture also integrates proven enterprise-level, Commercial-Off-The-Shelf (COTS) products.
- Centralized acquisition of site licenses for several key software components of the JCON system-The Program has taken advantage of the buying power of the combined JCON components to acquire discounted software and establish enterprise licenses for several key software products. The JCON PMO has established enterprise license agreements for file mirroring software, virus scanning software, security software (encryption) solutions, patch management, and automated forms processing. The program office spearheaded with Contract Management Services the Microsoft Global Enterprise Agreement<sup>8</sup> for all Microsoft licenses department wide. The program sponsors and maintains Bulk Purchase Agreements (BPAs) for desktop and laptop computers, printers, and IT services, all widely used by components.
- Consolidated contractual task orders such as Level IV support (i.e., senior technical support for problem resolution) made possible by the standard JCON operating system and messaging platform (Standard Architecture)-These tasks are a considerable economic savings for components that would otherwise have to purchase individual contracts at higher costs. An annual estimated cost savings of over \$1,000,000 is realized JCON-wide due to these collaborative efforts. Further consolidated savings occur with the volume discounts offered to the components through JCON-wide contract vehicles.
- Use of a standardized deployment methodology [i.e. System Development Life Cycle (SDLC)] to facilitate knowledge transfer, minimize technical risks, and reduce installation costs. The deployment methodology stipulates the steps needed to plan, design, test, and implement initial systems as well as subsequent architecture upgrades. As part of this methodology, the Program has developed standard documentation templates that are used by each component during their rollouts. These re-use results in significant cost and time savings by eliminating duplication of effort. Finally, this consistently results in the implementation of JCON systems on time and within budget.
- Maintenance of a Program-wide Configuration Management (CM) process ensures that consistent benefits (both technical and fiscal) are realized throughout the implementation of the JCON Standard Architecture-This CM process is used by the Program to manage problem identification, requirements tracking, and change control associated with the JCON Standard Architecture. Before any changes are made to the Standard Architecture, they are thoroughly tested in a laboratory environment by the PMO or a participating component to assure full system interoperability and compatibility. This approach ensures that modifications do not result in costly system failures or downtime.
- The JCONext infrastructure will enhance the JCON portfolio by introducing common end-user systems, centrally located and managed by a common JCONext Operations team. JCONext introduces a single domain where users and computers can be combined across components, yet maintains delegated administration authority so each component still “owns” and sees only their resources. Common systems, including Active Directory, SharePoint, Email and Blackberry are available for use by any component. The program will fund migrations into, and basic operations of the centralized services so that component CIOs in the 29 environments where IT operations are delegated, can focus component resources on mission activities rather than common, basic operations tasks.

---

<sup>8</sup> The Microsoft Enterprise Agreement has resulted in a one-time savings of approximately \$12.6 M for Program participants in 2001.

## Funding – JCON Program

### Base Funding

FY 2009 Enacted				FY 2010 Enacted				FY 2011 Current Services			
Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)
7		7	\$26,596	7		7	\$20,179	7		7	\$34,992

### Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Not Applicable				
Total Personnel				

### Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Total Non- Personnel	\$15,000	1	\$15,000	\$15,000

### Grand Total

	Pos	Agt/ Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)
Current Services	7		7	\$1,093	\$33,899	\$34,992
Increases					\$15,000	\$15,000
Grand Total				\$1,093	\$48,899	\$49,992

## VI. Program Increases

<b>Item Name:</b>	<b>Joint Automated Booking System (JABS)</b>
<b>Budget Decision Unit(s):</b>	JIST
<b>Strategic Goal(s) &amp; Objective(s):</b>	Strategic Goal 1 – Prevent Terrorism and Promote the National Security
<b>Organizational Program:</b>	JIST
<b>Component Ranking of Item:</b>	3 of 5

**Program Increase:** Positions 0 FTE 0 Dollars \$6,000,000

### **Description of Item:**

In FY 2011, the FBI will commence implementing the Next Generation Identification (NGI) system. This \$1 billion project will enhance its current Integrated Automated Fingerprint Identification System (IAFIS) capabilities while expanding into other forms of biometrics (i.e. palm prints, IRIS, facial recognition, etc.) JABS program currently accounts for 86% of the Federal electronic booking transactions submitted to IAFIS. This FY 2011 increase of \$6M to be recurred in FY 2012 through FY 2015, will allow the Joint Automated Booking System (JABS) to maintain compatibility with the FBI's biometric and criminal history data repositories and replace its obsolete fingerprint livescan devices. Over the next five fiscal years JABS will require \$30M, of which \$19M will be for software enhancements and \$11M for new biometric collection equipment. The total requested increase of \$30M (over five years) represents about 3% of the FBI's budget to implement NGI.

The JABS Program is a field-proven, mission critical law enforcement system responsible for capturing, processing, managing, and sharing detainee booking and tracking information. This Program provides the provisioning and operational maintenance for 1,100 Automated Booking Stations (ABS) within the DOJ and manages the electronic data interfaces with the FBI's IAFIS. Including booking stations maintained by DHS and the USMS's Inter-Agency booking functionality, JABS services approximately 2,500 Federal law enforcement sites. JABS, which operates 24/7, has an estimated 64,000 registered users who submit over 2 million transactions per year to IAFIS. These booking submissions provide a "real-time" updating of the FBI's fingerprint and criminal history databases.

JABS also provides booking information, including applicable scars, marks, and tattoo data, to counter terrorism and law enforcement fusion centers through OneDOJ. The JABS data repository currently consists of more than 3 million booking records which is cited by the law enforcement community as being extremely effective in accomplishing their mission. Additionally, JABS provides routine data extracts to the Organized Crime Drug Enforcement Task Force (OCDETF) fusion center, DEA- Pinellas County, FL Sheriff's Office facial recognition pilot fusion center, and the Arizona Counter Terrorism Information Center (ACTIC).

In FY 2008, the FBI started a \$1 billion ten-year project to replace its current system (IAFIS) with NGI. IAFIS is limited to using fingerprints as the primary biometrics for identification. NGI will expand biometrics analysis to a new level and allow law enforcement users to perform enhanced searches against the world's largest database of people's physical characteristics. When law enforcement officers detain a potential suspect, NGI will have the new capability to use palm prints, IRIS patterns, facial characteristics, and multimodal biometrics (fusion identification techniques using a combination of characteristics) to search for a match in the FBI database to determine if the individual is a terrorist, on the "most wanted" list, or has prior criminal offenses.

Coupled with the NGI initiative, the JABS Program must replace the ABS fingerprint livescan device. The technology refresh of the livescan equipment will be driven by and coordinated with the migration of the new biometrics features developed in Next Generation Identification (NGI). Since the program's inception, the JABS PMO has provided the ABS site equipment to the components. JABS has used the same livescan since FY 2001. The livescan vendor is no longer marketing this model of livescan device and will stop manufacturing it shortly because the machine's technology is outdated.

## **Justification:**

The DOJ law enforcement components rely on JABS for collecting biometric data, sending the data to the IAFIS/NGI repository, and sharing booking information to meet mission investigative and information sharing requirements. The use of IAFIS/NGI to support the Department's operational law enforcement responsibilities relies on its data repository being populated with a steady stream of biometric data from JABS.

The NGI compatibility and equipment refresh work needs to start in early FY 2011 to match the anticipated rollout of NGI. Evolution of JABS to be compliant with NGI involves:

- Modifying the JABS software to be compliant with the new standards used by NGI for exchanging biometric data. There will be unique standards for palm print data, for IRIS data, and for other biometrics.
- Integrating JABS with new peripheral hardware devices such as palm print scanners, IRIS scanners, and new cameras capable of taking facial-recognition-quality photographs. In addition the JABS is integrated with IAFIS. All of these software modules need to be upgraded.

To continue supporting 64,000 registered users as they perform the investigative and arrest responsibilities of DOJ and DHS law enforcement components, JABS must remain compatible with the advancements in biometric equipment associated with the NGI functionalities. This will require the purchase and installation of palm print scanners, IRIS scanners, and cameras at the DOJ's 1,100 ABS sites.

As a primary conveyor of booking and incarceration data to IAFIS, the FBI has sought the assistance of the JABS program to help populate their new database with new palm prints, IRIS scans, and facial recognition quality photographs. Simply put, the vision of NGI cannot be fulfilled for any users until the new database is populated with booking records that have new biometrics data.

## **Impact on Performance:**

As the primary source for Federal booking information to IAFIS/NGI, which is accessible to all Federal, state, and local law enforcement via OneDOJ, JABS must keep pace with the advancements in NGI data collection and information sharing technology. Maintaining the JABS capability to capture, process, manage, and share booking related information is essential in supporting the Department's law enforcement components.

Failure to effectively comply with the transaction and associated equipment changes developed in NGI will:

- Adversely impact JABS ability and reduce its operational effectiveness to support proper electronic submission of improved booking and incarceration data to NGI.
- Reduce the number and types of investigative information available to the DOJ law enforcement components.
- Restrict the types and quality of data available to all law enforcement organizations via OneDOJ since JABS is a major data contributor to OneDOJ.

Failure to deal with the existing equipment obsolescence will result in the following operational issues:

- Increase the booking process time and reduce the quality of fingerprint capture by requiring the officer to manually "ink" a fingerprint card and then scan the prints into the JABS transaction. Note: scanned fingerprint data has a significantly higher IAFIS rejection rate versus the electronically captured fingerprint data.
- Significantly decrease the percentage of DOJ's arrest transactions submitted electronically to IAFIS from its current rate of 99%. Note: manual transactions significantly increase the time (weeks vs. minutes) to identify an individual and to make the arrest data available to all levels of law enforcement (federal, state, and local.)

JABS must begin the development and equipment procurements associated with NGI initiative in FY 2011 to ensure that it continues to support the Department's law enforcement tasks.

## **Funding – JABS Program**

### Base Funding

FY 2009 Enacted			FY 2010 Enacted			FY 2011 Projected		
Pos	FTE	\$000	Pos	(\$000)	(\$000)	Pos	FTE	\$000
7	7	9,006	7	7	\$9,600	7	7	13,715

### Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from FY 2010) (\$000)
Total Personnel	0	0	\$0	\$0

### Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request (\$000)	FY 2012 Net Annualization (Change from FY 2011) (\$000)
Total Non-Personnel	\$6,000	1	\$6,000	0

### Total Request for this Item

	Pos	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)
Current Services	7	7	\$ 985	\$ 12,730	\$ 13,715
Increases	0	0	\$ 0	\$ 6,000	\$ 6,000
Grand Total	7	7	\$ 985	\$18,730	\$ 19,715



**Item Name:** **Unified Financial Management System (UFMS)**

Budget Decision Unit(s): JIST  
Strategic Goal(s) & Objective(s): Strategic Goal 3: Ensure the Fair and Efficient Administration of Justice  
Organizational Program: JIST

Component Ranking of Item: 4 of 5

Program Increase: Positions 11 FTE 5.5 Dollars \$42,132,000

**Program Background**

Identified by the Department's Inspector General as "one of the most important challenges for the Department," the Department is implementing a Unified Financial Management System (UFMS) that will replace legacy financial systems operated by individual components. The UFMS will replace six (6) core financial management systems and multiple procurement systems currently operating across the Department with an integrated Commercial Off The Shelf (COTS) solution. This will allow the Department to streamline and standardize business processes and procedures across all Components, providing accurate, timely, and useful financial data to financial and program managers across the Department, and produce Component and Department level financial statements. In addition, the system will assist the Department by improving financial management performance and aid in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security identified by the Department's Inspector General. UFMS directly supports the Attorney General's top priority to "ensure the transparent, accountable, and depoliticized administration of justice." UFMS also directly supports Strategic Goal 3: Ensure the Fair and Efficient Administration of Justice included in the Department's Strategic Plan, FYs 2007 – 2012.

The UFMS will allow the DOJ to streamline and standardize business processes and procedures across all components, providing secure, accurate, timely, and useful financial and procurement data to program managers across the Department, and produce component and Department level financial statements. In addition, the system will assist the DOJ by improving procurement and financial management performance and aid department components in addressing the material weaknesses and non-conformances in internal controls, accounting standards, and systems security. Finally, the system will provide fully integrated financial and procurement functionality to streamline business processes, provide consolidated management information, and the capability to meet all mandatory requirements of the Federal Acquisition Regulation (FAR) and the Justice Acquisition Regulations (JAR).

UFMS will ensure that uniform and centralized data is readily available. The capability of UFMS to present information in a consistent, predictable manner reduces the need for data comprehension, and directly impacts the time required to prepare reports based on Component information.

The UFMS program is centrally managed by the UFMS Program Management Office (PMO) within the Controller's Staff of the Justice Management Division. The program office provides overall program management, technical direction and oversight, project controls, and serves as the central coordination point for all program activities.

**Major FY 2010 Activity**

FY 2010 is another crucial year for the implementation of UFMS. Major activities planned for FY 2010 include: (1) completion of the UFMS 2.0 upgrade; (2) completion of U.S. Marshals Service (USMS) implementation of UFMS Acquisitions (phase 1); (3) finalize the ATF requirements and testing (for go-live in first quarter of FY 2011); (4) initiate planning for the final phase of the USMS implementation; and, (5) initiate FBI phase 2 gap analysis and requirements. The Program is awaiting congressional approval of a reprogramming notification for \$114.7M which will fund the FY 2010 implementation activities.

The FY 2010 notification includes \$44.0 million for FBI Phase 2 implementation which includes defining requirements, reengineering business processes, configuring, testing, developing training materials and implementing the Criminal Justice Information System (CJIS) and a few other small organizations. Phase 2 also involves the stand up of the SECRET infrastructure. Phase 3 involves updates to all of the above based on the results of the Phase 2 implementation, and also includes increased hardware capacity, training and full implementation to the remaining FBI users. The notification includes \$16.6 million for FBI Phase 3 implementation activities to be completed in FY 2013.

The USMS will implement Phase 1, UFMS Acquisitions, in FY 2010, demonstrating that both BOP and USMS can successfully share and operate in a single instance. This effort avoids a planned expense by USMS to acquire an interim solution for automated acquisition support, and will better prepare USMS for the full deployment of UFMS. Also during FY 2010, USMS planning will commence including requirements gathering and gap analysis for full implementation of UFMS. The notification includes \$22.1 million to complete the USMS implementation which is scheduled to be completed by the 2<sup>nd</sup> quarter of FY 2012.

\$17.0 million of the reprogrammed funds will enable the UFMS program office to maintain adequate staffing levels necessary for program management and oversight of the critical activities noted above. The program office serves as the central coordination point for all program activities to ensure successful system implementations throughout the Department. The \$17 million is in addition to the program's FY 2010 base resources of approximately \$21 million which will be utilized to fund the UFMS program annual fixed costs which include rent, utilities, telecommunications, hardware and maintain current staffing to manage the schedule, budget, deliverables, program risks, functional and technical activities of the program. The PMO provides guidance to assist with the coordination and oversight of program resources to ensure successful system implementations throughout the Department. This also includes providing management oversight and direction to the Operations and Maintenance activities.

\$15.0 million of the reprogrammed funds will be carried forward to FY 2011 in an effort to sustain funding levels for base resources which were increased during FY 2010 for the UFMS program annual fixed costs. The PMO requires the additional funding to continue to provide the guidance necessary to assist multiple components with the coordination and oversight to achieve successful system implementations throughout the Department.

### **FY 2011 Program Increase Justification**

UFMS is requesting a program increase of 11 positions and \$42.132 million. This includes \$787,000 in personnel costs for the 11 new positions. Including the \$15 million carryover funding from the FY 2010 reprogramming noted above, the total budget available to UFMS in FY 2011 is \$57.132 million.

This enhancement request includes \$22.963 million to complete the Bureau of Prison's (BOP) UFMS implementation. This includes comprehensive planning and requirements gathering to support the full integrated implementation of UFMS to BOP. The request also funds the design, development, configuration, data conversion, testing, and the incremental deployment of UFMS functionality to the BOP. For example, the enhancement will allow the BOP to expand the use of UFMS Acquisitions to provide the Bureau Program Managers with the capability to submit requisition requests to the procurement staffs for processing. This increment would add about 3,000 additional users to UFMS and put the BOP in a better position to implement the entire financial user community. The planning materials will be leveraged during the implementation phase and will include the Project Management Plan, Project and Risk Management Plans, Concept of Operations Document, Data Conversion Plan and Analysis, Business Process Maps and Data Dictionaries, Security Requirement Plan, Requirements, and System Implementation Plans. It is anticipated that the remainder of the funding needed to complete the Department's Offices, Boards and Divisions (OBDs), including the Office of Justice Programs (OJP), will be acquired through a reprogramming request, similar to past funding practices.

This enhancement request will also restore base funding to allow the UFMS Program Management Office (PMO), working with the Implementation and Integration (I&I) contractor, to initiate and complete a majority of

the following implementation activities such as Project Management, Business Process Re-engineering/Change Management, Configuration Activities, Data Cleanup and Conversion Activities, Integration and Interface Design activities, Testing activities, Training activities. Restoration of base funding is critical in FY 2011 as the program will be challenged with multiple component implementations. As noted, the program will be simultaneously implementing USMS and FBI, and initiating a new implementation for BOP. Also, pending the availability of internal resources, the Department intends to submit a reprogramming request for the last remaining components, that being the OBDs and OJP. With this in mind, it is critical that base resources are available to the program to manage the remaining critical priorities, resolve technical issues, and enhance the system as necessary so that the vision of a single procurement and financial/accounting system is realized. This includes fixed costs such as engineering support to ensure the development and maintenance of the core financial application. Base funding will help cover the development, testing, and building of interim and final releases for Foundation Build and Component builds that incorporate problem reports and/or Change Control Board approved change requests into the product baselines. The funding will also be utilized to cover costs for internal help desk and operations support within the non-production O&M support.

The FY 2011 non-personnel increase will fund contractors responsible for the design, development, configuration, data conversion, testing, and the incremental deployment of UFMS functionality to the BOP. User licenses and related software purchases are also included as part of the requested increase.

The PMO is currently authorized 14 positions for FY10 in the JIST appropriation. The enhancement requested will bring the PMO to 25 authorized positions. This is a modest increase in lieu of the multiple priorities being addressed in FY 2011. The additional resources will help the program manage the final phases of the implementations within the timeline goals of the program. It is critical that the program stay on schedule with the implementations if the program costs are to remain under budget. The additional personnel resources will help ensure goals are realized within the prescribed schedule timeline. This level of direct government effort is predicated on the judicious use of contractor personnel. GAO and other third party studies of federal financial management systems projects clearly indicate the need for significant levels of government resources for success. Over reliance on contractor support has been identified as a cause of difficulties encountered in projects similar to the DOJ UFMS.

### **Impact on Performance**

DOJ took a major step toward a new and more efficient way of managing its fiduciary responsibilities by implementing UFMS as the system of record for DEA in January 2009. In addition, the Bureau of Prison (BOP) UFMS Acquisitions implementation achieved “Go Live” status in June 2009. The PMO is scheduled to implement the United States Marshals Service (USMS) Acquisitions during the 2<sup>nd</sup> quarter of FY10 and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) full deployment during 1<sup>st</sup> quarter FY11.

Some of the key positive performance objectives that will be optimized at each DOJ component will be:

- Reduction in manual and duplicative transaction processing efforts - UFMS integrates the acquisition process with finance which means much of the data is entered once and then used many times as the requisition is reviewed/approved, goods or services are acquired/received and invoices are paid. This improves productivity and ensures less opportunity for errors. Prior to UFMS, DEA had an automated acquisition system that was NOT integrated with finance which required duplicate/redundant data.
- Effectively use technology with advanced controls for auditing, data integrity and interfaces that support financial and procurement transactions - Improved internal controls delivered systemically by UFMS provide edits/defaults to improve productivity, reduce errors and provide documentation/audit trails that can help to identify gaps, weaknesses and thereby reduce fraud, waste and abuse.
- Reduction in errors in financial and procurement transaction processing.

- Timely financial reporting - Improved efficiency and effectiveness of the DOJ's financial management and reporting capabilities.
- Improved efficiency and effectiveness of the Department's funds management - Automated reconciliation and fund control capabilities also improve productivity and minimize risks.
- Increase ability to pay invoices on time.
- Improved efficiency and effectiveness of the DOJ's asset management.
- More modern security tools and practices.
- Reduced audit effort and costs - Long term efficiencies will be realized in the areas of automated financial statement preparation and the financial audit efforts. The decentralized nature of the Department's financial management is the driving force behind the current process of completing component audits that are then rolled up into the consolidated Departmental audit. The number of financial management systems and data centers used by the Department's reporting entities limits the options that could be implemented to achieve future cost savings or at least continue to reduce the level of effort. According to the OIG, the Department spent over \$11 million on 81,000 contract labor hours for the FY 2008 audit process and a comparable amount for the FY09 audit.

In order to accomplish its mission effectively, the UFMS PMO requires subject matter experts and managers with deep seeded knowledge, skills, and abilities in their specific roles and responsibilities. The requested enhancement for eleven (11) positions will fill a subject matter knowledge and/or project management gap in the following critical areas:

- Implementation Leads (3 positions)
- IT Manager (1 position)
- Business Transformation Manager (1 position)
- IT Security Specialist (1 position)
- Contract Specialist (1 position)
- PMO Support Staff (4 positions)

## Funding - UFMS

### Base Funding

FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Pos	Agt/Atty	FTE	\$(000)	Pos	Agt/Atty	FTE	\$(000)	Pos	Agt/Atty	FTE	\$(000)
14			\$21,132	14			\$21,132	14			\$0

### Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
GS-15		3	\$242	\$133
GS-14		7	\$486	\$267
GS-13		1	\$59	\$32
<b>Total Personnel</b>		<b>11</b>	<b>\$787</b>	<b>\$432</b>

### Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request (\$000)	FY 2012 Net Annualization (Change from 2011) (\$000)
Contractors and Software	\$38,834	1	\$38,834	
<b>Total Non-Personnel</b>	<b>\$38,834</b>		<b>\$38,834</b>	

### Total Request for this Item

	Pos	Agt/Atty	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)
Current Services	14		14	\$[2,511]	\$[18,621]	\$[21,132]
Increases	11		6	\$3,298	\$38,834	\$42,132
<b>Grand Total</b>	<b>25</b>		<b>20</b>	<b>\$3,298</b>	<b>\$38,834</b>	<b>\$42,132</b>

## VI. Program Increases

**Item Name:** JCON-Secret and JCON-Top Secret (JCON-S/TS)

**Budget Decision Unit(s):** JIST

**Strategic Goal(s) & Objective(s):** Strategic Goal 1 – Prevent Terrorism and Promote the National Security  
Strategic Goal 2 – Prevent crime, enforce federal laws, and represent the rights and interest of the American People.  
Strategic Goal 3 – Ensure the fair and efficient administration of justice.

**Organizational Program:** JIST

**Component Ranking of Item:** 5 of 5

**Program Increase:** Positions 0 FTE 0 Dollars \$4,300,000

### **Description of Item:**

This FY 2011 funding increase of \$4,300,000 recurred as an increase to the JIST base appropriation, will allow the JCON-Secret and JCON-Top Secret Program (JCON-S/TS) to implement critical improvements to the JCON-S/TS systems to provide the increased level of performance required to support the legal and investigative component users in the direct support of the Department's Counter Terrorism, Counter Espionage, Investigative, Enforcement and Prosecutorial missions. The JCON-S/TS provides the most comprehensive-widely used classified system by the Department and its components to process Secret and Top Secret - Sensitive Compartmented Information (TS/SCI). These systems are critical to highest Strategic Goals of the Department. The JCON-S/TS systems are used by the Department; its components and other federal agencies at over 400 locations within the United States and associated U.S. Territories from the Virgin Islands to Guam.

This funding will increase the effectiveness of the JCON-S/TS Systems to provide critical services to Department through the following initiatives:

- Implement Thin Client to provide users with an industry recognized solution to increase system performance.
- Modernize encryption by replacing old generation communication security encryption devices (Taclanes) with new equipment that match the performance of other equipment in the network.
- Improve data storage capabilities to increase file access performance and reliability
- Upgrade the network infrastructure components supporting the larger user sites to provide increased processing capabilities and throughput.

Once JCON-S/TS achieves its system performance targets, the following initiatives could be undertaken to enhance direct support of Department's Counter Terrorism, Counter Espionage, investigative, Enforcement and Prosecutorial missions:

- Enhance Information Sharing Capabilities and Collaboration through the establishment of Community of Interest and Portals
- Provide expanded service to Department Components and Intelligence Community Partners
- Enhance Continuity of Government (COG) and Continuity of Operations (COOP) capabilities
- Implementation of Investigative Tools, Datasets and services to enhance the counterterrorism/counterespionage missions

## **Justification:**

Established at the direction of the Attorney General, the initial JCON-S/TS mission was to establish secure intra/inter-departmental classified data and communication networks that did not exist on 9/11/2001. The JCON-S/TS fulfilled that directive and currently provides Secret and Top Secret/SCI service to all of the Department's components along with Other Government Agencies.

As the demand for this service continues to grow, these systems are now the primary tool used across the Department and its components to communicate and process classified information electronically. During the past five years, the Department has experienced a twenty-fold increase in the amount of classified information received and processed from outside agencies. This increase has exposed an immediate and critical need to improve infrastructure so that it can sufficiently process the additional workload and is the primary purpose of this funding request. Failure to do so could effect system reliability and have downstream impacts on counterterrorism and prosecutorial efforts.

The JCON-S/TS was formally established as a program in FY 2005 and has received limited funding during the subsequent FYs. During that time, the JCON-S/TS have experienced rapid growth as reflected in the number of users and workstations deployed. Currently there are over 1,000 deployed workstations supporting over 3,000 users at over 400 locations within the Continental United States (CONUS) and other U.S. Territories (OCONUS) such as Alaska, Hawaii, Guam, and the U.S. Virgin Islands. Since the inception of the program, JCON-S/TS systems have been a critical element of the Department's Continuity of Government (COG) and Continuity of Operations (COOP).

JCON-S/TS have experienced considerable success in providing the Secret and Top Secret/SCI systems to the Department and its components. This includes instances requiring rapid deployment of infrastructure to support the Presidential Detention Task Forces and Guantanamo Bay Litigation, among others.

Another element of this request is to improve information sharing and collaboration capabilities through implementation of portals/communities of interest (COI) – thus providing tools enabling intelligence information to be shared among key stakeholders. Sharing of information, especially with intelligence partners, is key and critical to combating terrorism, completing successful apprehensions and subsequent prosecutions.

In addition to Collaboration and Information Sharing tools, the components leveraging JCON-S/TS systems in support of their mission need additional Investigative Tools and Datasets to support the ever increasing complexity and volume of information. Intelligence analysts and field law enforcement must quickly be able to process vast amounts of information using tools that link common elements (people, places, associations, etc.). This request is to implement broad-based intelligence link analysis tools for DOJ components.

The above JCON-S/TS enhancements are necessary to continue to meet the needs of the Department and its components in the attainment of agency goals and directives. The program has reached a point where these systems are in need of modernization to ensure the systems and tools are in place to support the stated Departmental goals and objectives along with COG and COOP activities.

## **Impact on Performance:**

The ability of the Classified Information Technology Program to support the Department and its components in achieving the strategic goals of preventing terrorism and promoting the national security depends heavily on its capability to capture, process, manage, analyze, and share information. DOJ Components have come to rely on the systems provided by JCON-S/TS to provide this service. These enhancements will better support the Strategic Goals of the Department while ensuring that these systems continue to provide the user with the best technology and ensure the security of these systems and data.

## **Funding – JCON-S/TS**

### Base Funding

FY 2009 Enacted				FY 2010 President's Budget				FY 2011 Current Services			
Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)	Pos	Agt/ Atty	FTE	(\$000)
3		3	\$5,451	3		3	\$5,500	3		3	\$5,560

### Personnel Increase Cost Summary

Type of Position	Modular Cost per Position (\$000)	Number of Positions Requested	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Total Personnel				

### Non-Personnel Increase Cost Summary

Non-Personnel Item	Unit Cost	Quantity	FY 2011 Request (\$000)	FY 2012 Net Annualization (change from 2011) (\$000)
Total Non-Personnel	\$4,300	1	\$4,300	\$0

### Grand Total

	Pos	FTE	Personnel (\$000)	Non-Personnel (\$000)	Total (\$000)
Current Services	3	3	\$585	\$4,975	\$ 5,560
Increases				\$4,300	\$ 4,300
Grand Total	3	3	\$585	\$9,275	\$9,860